Deutscher Bundestag **Drucksache 19/12489**

19. Wahlperiode 19.08.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Britta Haßelmann, Agnieszka Brugger, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/11754 –

Aktivitäten der Bundesregierung gegen illegitime Beeinflussung demokratischer Willensbildungsprozesse

Vorbemerkung der Fragesteller

Die große Stärke westlicher Demokratien sind ihre offenen und pluralistischen Gesellschaften. Genau diese aber bieten auch vielfältige Angriffsflächen und sind damit in besonderem Maße durch hybride Aktivitäten verwundbar.

Belege gibt es genug: Für Einflussnahmen im Vorfeld und im Kontext demokratischer Wahlen (US-Wahl, www.tagesschau.de/ausland/einflussnahme-us-wahl-101.html; Brexit, www.deutschlandfunk.de/soziale-medien-und-das-brexit-referendum-propaganda-luegen.724.de.html?dram:article_id=430936) oder Referenden (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018R0842&from=DE), weitreichende IT-Angriffe auf Politikerinnen und Politiker (IT-Angriff auf den Bundestag www.tagesschau.de/thema/bundestag/index.html Doxing-Fall www.zeit.de/digital/datenschutz/2019-01/privatsphaere-doxing-daten-sammeln-datensicherheit-politiker), Medien (www.haz.de/Nachrichten/Digital/Verfassungsschutz-warnt-vor-Cyber-Angriffen-auf-deutsche-Medienhaeuser) sowie demokratische Institutionen. Auch die intransparente Verbreitung von Falschnachrichten mit dem Ziel, demokratische Diskurse bewusst zu manipulieren, das Vorgaukeln von Diskursmacht im Digitalen durch Bots und ganze Troll-Armeen oder die bewusste Parteinahme und Unterstützung politischer Kräfte, die das Ziel verfolgen, öffentliche Diskurse zu vergiften und die Demokratie in Frage zu stellen (www.zeit.de/politik/ausland/2018-12/us-wahl-2016-russland-einmischung-soziale-medien) – all dies sind Phänomene einer neuen hybriden Bedrohungslage über die gesamtgesellschaftlich seit Langem diskutiert wird, ohne dass die Bundesrepublik Deutschland nach Ansicht der Fragesteller bisher ihrem Anspruch einer wehrhaften Demokratie adäquat gerecht geworden wäre und Antworten auf diese neuen Strategien bewusster Destabilisierung und Zersetzung gefunden hätte.

Während in anderen Ländern und auf Ebene der Europäischen Union Politik und Zivilgesellschaft versuchen, zurückliegende Einflussnahmen und Manipulationsversuche (https://ec.europa.eu/germany/news/20181126-umfrage-einflussnahme-auf-wahlen_de) zu analysieren und intensiv an Gegenstrategien

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 14. August 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

gearbeitet wird, bleiben vergleichbare Handlungen von Seiten der Bundesregierung nach Ansicht der fragestellenden Fraktion bislang weitgehend aus. Trotz zahlreicher Hinweise auf weitreichende Manipulationsversuche staatlicher und nichtstaatlicher Akteure, trotz nachgewiesener Versuche bewusster Diskursverschiebungen im Zuge von (Landtags-)Wahlen, beispielsweise durch rechte Netzwerke (www.br.de/nachrichten/bayern/kampf-um-bayern-online-kampagnen-zur-landtagswahl-2018,RI7e9qg), trotz erfolgreicher IT-Angriffe auf Privatpersonen und demokratische Institutionen wie den Deutschen Bundestag, trotz durch Medienberichte aufgedeckter Einflussnahmen auf Abgeordnete des Deutschen Bundestages, die nach Angabe ausländischer Akteure unter „totaler Kontrolle" stehen (vgl. DER SPIEGEL 6. April 2019), trotz massiver Stimmungsmache in erfundenen Fällen wie dem sogenannten Fall Lisa (www.spiegel.de/politik/ausland/russland-deutsche-geheimdienste-werfen-moskau-gezielte-stimmungsmache-vor-a-1129853.html) durch ausländische Regierungen, trotz einer an Intensität zuletzt stark zugenommenen öffentlichen Debatte über diese Problemlagen (www.gruen-digital.de/2018/11/6-netzpolitische-soire-hacked-democracy-demokratie-schuetzen-am-4-dezember-in-berlin/) und trotz vielfacher Warnungen von Seiten der Nachrichtendienste vermisst die fragestellende Fraktion noch immer die notwendige Sensibilität auf Seiten der Bundesregierung.

Wenn bewusst und intransparent Zweifel gesät werden und wenn versucht wird, das Vertrauen in öffentliche Debatten, in demokratische Wahlen und auch in die internationale Kooperation von Staaten zu untergraben, braucht es nach Ansicht der Fragesteller nationale und internationale Gegenstrategien.

Auch zahlreiche parlamentarische Nachfragen im Deutschen Bundestag, vorgelegte Initiativen (vgl. exemplarisch Anträge der Fraktion BÜNDNIS 90/DIE GRÜNEN „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern" auf Bundestagsdrucksache 19/1328 und „Für wehrhafte Demokratien in Europa – Rechtsstaatlichkeit und Grundrechte in den Mitgliedsländern der EU stärken" auf Bundestagsdrucksache 19/7436) und durch die Fachausschüsse durchgeführte Expertengespräche (www.bundestag.de/ausschuesse/a23_digital/anhoerungen#url=L2F1c3NjaHVlc3NlL2EyM19kaWdpdGFsL2FuaG9lcnVuZ2VuL2FuaG9lcnVuZy01OTIzNzA=&mod=mod557988) haben bislang nicht dazu geführt, dass die Bundesregierung sich nach Meinung der fragestellenden Fraktion der Problematik mit der notwendigen Ernsthaftigkeit zugewendet und entsprechende Gegenstrategien für diese unterschiedlich gelagerten Phänomene und Problemlagen entwickelt hätte.

Bei der Abwehr hybrider Bedrohungen sind aus demokratischer Sicht gewichtige Güterabwägungen zu treffen. Im Bereich der Bekämpfung von Desinformation geht es oftmals nicht um eindeutig rechtswidrige Inhalte wie Volksverhetzung oder den Aufruf zu Straftaten, sondern nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können. Hier muss aus Sicht der Fragesteller ein Gleichgewicht gefunden werden zwischen der Notwendigkeit, Bürgerinnen und Bürger sachlich korrekt zu informieren, und dem Recht auf freie Meinungsäußerung. In Aussicht gestellte Maßnahmen wie beispielsweise veränderte Strukturen zur verbesserten Erkennung neuer hybrider Bedrohungen wurden aus Sicht der Fragesteller bislang nicht angegangen.

Während die EU-Kommission sich seit Jahren mit den neuen hybriden Bedrohungen beschäftigt und im Vorfeld der kommenden Europawahlen einen entsprechenden Aktionsplan zum Schutz (https://eeas.europa.eu/headquarters/headquarters-homepage/56267/aktionsplan-gegen-desinformation_de) derselben verabschiedet hat, vermisst die fragestellende Fraktion eine angemessene Beschäftigung mit der Thematik seitens der Bundesregierung bis heute. Eine solche ist allerdings angesichts der relevanten Gefahr für demokratische Diskurse auch sicherheitspolitisch dringend geboten.

Vorbemerkung der Bundesregierung

1. Der Begriff der „hybriden Bedrohungen“ wird unterschiedlich verstanden. Die Europäischen Kommission versteht unter hybriden Bedrohungen die Mischung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden, auf die von staatlichen oder nichtstaatlichen Akteuren in koordinierter Weise zur Erreichung bestimmter Ziele zurückgegriffen wird, ohne dass jedoch die Schwelle eines offiziell erklärten Kriegs erreicht wird. Ziel ist dabei nicht nur, unmittelbaren Schaden anzurichten und Verwundbarkeiten auszunutzen, sondern auch Gesellschaften zu destabilisieren und durch Verschleierungstaktik die Entscheidungsfindung zu behindern. Im Übrigen wird auf die Vorbemerkungen in den Antworten zu den Kleinen Anfragen der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/8631 und der Fraktion der AfD auf Bundestagsdrucksache 19/1262 Bezug genommen.

Nach diesem Verständnis können grundsätzlich viele Vorkommnisse, mit dem Potenzial die Gesellschaft zu destabilisieren oder die politische Entscheidungsfindung zu behindern, Teil einer hybriden Kampagne sein.

Entsprechend sind hybride Bedrohungen keine neue Erscheinung. Globalisierung und moderne Informationstechnologien haben jedoch zahlreiche Interventionsmöglichkeiten geschaffen, die kostengünstig sind und sich durch schier unbegrenzte Reichweite auszeichnen. Zudem tragen die Veränderungen der sicherheitspolitischen und strategischen Lage dazu bei, dass liberale Demokratien sich hybrider Bedrohungen stärker als zuvor ausgesetzt sehen. Die Bundesregierung nimmt daher hybride Bedrohungen sehr ernst und ist für die daraus erwachsenden Gefahren hochgradig sensibilisiert. Entsprechend hat die Bundesregierung in der Vergangenheit intern aber auch auf europäischer und internationaler Ebene an der Bekämpfung hybrider Bedrohungen und der Erhöhung der Resilienzen gearbeitet. So nahm sie unter anderem an dem Workshop auf EU-Ebene aktiv teil, der zum Ergebnis den vom Fragensteller erwähnten Aktionsplan der Europäischen Kommission zum Schutz der Europawahlen hatte.

2. Daneben hat die Bundesregierung auch intern das Thema weiter forciert. So hatte sie bereits im Jahr 2016 nach der Veröffentlichung der Gemeinsamen Mitteilung des Europäischen Auswärtigen Dienstes (EAD) und der EU-Kommission vom 7. April 2016 und den Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen vom 19. April 2016 hierzu interimsweise ein ressortübergreifendes Netzwerk „Hybride Bedrohungen“ eingerichtet. Im September 2018 wurde die ressortübergreifende „Arbeitsgruppe zur Strategischen Koordination des Umgangs mit Hybriden Bedrohungen“ geschaffen und das frühere Netzwerk hierein überführt. Seit Juli 2019 hat zudem das Bundesministerium des Innern, für Bau und Heimat (BMI) die ressortübergreifende Federführung für das Thema übernommen. Das BMI setzt im Rahmen der Koordinierung einen regierungsweiten Ansatz um. Demnach sollen alle Ministerien und Behörden in die Abwehr hybrider Bedrohungen eingebunden werden. Hybride Bedrohungen orientieren sich an den Vulnerabilitäten der Gesellschaft und des Staates. Diese begrenzen sich grundsätzlich nicht auf die Zuständigkeit einzelner Ministerien. Im Rahmen des regierungsweiten Ansatzes prüft das BMI auch, ob die bestehenden Strukturen diesem Ansatz gerecht werden.

3. Der von den Fragestellern verwendete Begriff „Hackback“ wird von der Bundesregierung konzeptionell nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage legt die Bundesregierung insoweit die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung zur Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 zugrunde.

1. Sieht sich die Bundesregierung weiterhin lediglich „Desinformations- und Propagandamaßnahmen“ und keinen belegbaren „hybriden Bedrohungen“ ausgesetzt (vgl. u. a. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN „Rechtspopulismus, Rechtsextremismus und Politische Desinformation im Netz“ auf Bundestagsdrucksache 19/2224 sowie die Antwort auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388) oder liegen der Bundesregierung mittlerweile Erkenntnisse für den Einsatz darüber hinausgehender hybrider Kampagnen in Deutschland vor, und für wie groß hält die Bundesregierung die derzeitige Bedrohung durch hybride Kampagnen insgesamt?

Die Bewertung der Bundesregierung in den in Bezug genommenen Antworten hat weiterhin Bestand. Ergänzend wird auf die Antwort zu den Fragen 1 und 2 der Kleinen Anfrage der Fraktion der AfD „Hybride Bedrohungen“ auf Bundestagsdrucksache 19/1262 hingewiesen. Über die in diesen Anfragen enthaltenen Informationen hinausgehend liegen der Bundesregierung keine Erkenntnisse zum Einsatz hybrider Mittel oder Kampagnen in Deutschland vor. Gleichwohl schätzt die Bundesregierung die potenzielle Bedrohung Deutschlands durch hybride Bedrohungen nach wie vor als hoch ein.

2. Liegen der Bundesregierung gegenwärtig konkrete Erkenntnisse bezüglich gezielter Beeinflussungsmaßnahmen der EU-Wahlen 2019 bis hin zu aggressiven Cyberkampagnen (APTs) durch Drittstaaten vor, und wenn ja, welche?

Die Europäische Kommission hat in dem am 14. Juni 2019 veröffentlichten Bericht über die Umsetzung des Aktionsplans gegen Desinformation (JOIN (2019) 12 final) festgestellt, dass keine speziell auf die Europawahlen ausgerichtete Desinformationskampagne aus externen Quellen ausgemacht werden konnte. Allerdings hätten unter anderem russische Quellen fortlaufend Desinformation betrieben, deren Zielsetzung in der Senkung der Wahlbeteiligung sowie der Einflussnahme auf den Wählerwillen bestand. Die Erkenntnisse der Bundesregierung decken sich mit dem genannten Bericht der Europäischen Kommission.

Darüber hinaus liegen der Bundesregierung derzeit keine Erkenntnisse zu aggressiven Cyberkampagnen (APTs) durch Drittstaaten zur gezielten Beeinflussung der EU-Wahlen 2019 vor.

3. Welche Vorkommnisse der vergangenen fünf Jahre zählt die Bundesregierung als Elemente einer hybriden Bedrohung und/oder Bestandteil hybrider Kampagnen?

Es wird auf die Antwort zu Frage 1 verwiesen.

4. Welche Position vertritt die Bundesregierung im Hinblick auf den Vorschlag der EU-Kommission für die Schaffung nationaler Netze der Zusammenarbeit bei Wahlen speziell im Hinblick auf Wahlfragen, IT-Sicherheit, Datenschutz, Strafverfolgung usw. (vgl. PM EU-KOM vom 29. Januar 2019, IP/19/746), und welche Behörde soll als Kontaktstelle für ein europäisches Kooperationsnetz für Wahlen benannt werden?

Als nationale Kontaktstelle für das europäische Wahlkooperationsnetzwerk im Sinne der Empfehlung der Europäischen Kommission C (2018) 5949 vom 12. September 2018 wurde bereits am 18. November 2018 die im BMI für die Europawahl sowie das deutsche und europäische Wahl- und Parteienrecht zuständige Arbeitseinheit benannt.

Im Übrigen wird auf die Antworten der Bundesregierung auf die Schriftliche Frage 39 der Abgeordneten Renate Künast auf Bundestagsdrucksache 19/6511 und auf die Schriftliche Frage 27 der Abgeordneten Dr. Franziska Brantner auf Bundestagsdrucksache 19/6961 sowie auf die Antwort der Bundesregierung auf die Mündliche Frage 48 der Abgeordneten Renate Künast in der Fragestunde vom 16. Januar 2019 (Plenarprotokoll 19/73) verwiesen.

5. Welche konkreten Möglichkeiten unterstützt die Bundesregierung für die verstärkte Beteiligung der Forschung, um Ausbreitung und Auswirkungen von Desinformation besser nachvollziehen zu können?

Forschung zu Verbreitung und Wirkung ist eine zentrale Voraussetzung für den richtigen Umgang mit Desinformation. Die Bundesregierung unterstützt die Beteiligung von Forscherinnen und Forschern mit dem Ziel, ein besseres Verständnis der Thematik zu erlangen und effektivere Maßnahmen ergreifen zu können. Das Auswärtige Amt hat beispielsweise die NRO Democracy Reporting International bei der Durchführung von zwei Workshops finanziell unterstützt und somit zur besseren Vernetzung von relevanten Akteuren vor und nach der Wahl zum Europäischen Parlament 2019 beigetragen.

Im nachgeordneten Bereich des Bundesministeriums der Verteidigung (BMVg), im Kommando Cyber-/Informationsraum, wird eine Studie im Rahmen eines Entwicklungsprojekts „Propaganda Awareness“ durchgeführt.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert Forschungsvorhaben, in denen die Auswirkungen neuer technischer Möglichkeiten für gezielte Desinformation, versteckte Propaganda bis hin zu koordinierten Kampagnen analysiert werden. Das Forschungsprojekt PropStop hatte zum Ziel, Desinformationen mit Fokus auf sogenannte Social-Bots zu erkennen und im nächsten Schritt diese Informationen zu bekämpfen. Das Projekt DORIAN untersucht darüber hinaus das Spannungsfeld zwischen freier Meinungsäußerung, Schutz der Privatheit und Zensur. Ein Teilziel ist hierbei die automatisierte Erkennung von Desinformation, bei der unter anderem Beiträge im Vorfeld der Europawahl untersucht worden sind. Das Forum Privatheit, eine interdisziplinäre Forschungs- und Dialogplattform, gestaltet zudem einen breiten Dialog zur zunehmenden Digitalisierung unserer Gesellschaft. Hier wird diskutiert, wie sich aus der gezielten Manipulation von online-Beiträgen Verwundbarkeiten ergeben, denen sich Gesellschaft, Wirtschaft und Politik stellen müssen. Der Bereich Demokratie, Partizipation und Öffentlichkeit ist eines von sechs Themenfeldern des BMBF-geförderten Weizenbaum-Instituts für die vernetzte Gesellschaft. Erforscht werden Wechselbeziehungen zwischen Digitalisierung und Selbstbestimmung, Inhalte und Prozesse politischer Kommunikation in digitalen Öffentlichkeiten mit Blick auf die Verbreitung von extremistischen Ansichten, Gerüchten und Lügen oder

die Rolle von digitalen Technologien und Medien bei der Entstehung von (trans-)nationalen Öffentlichkeiten, Kommunikationsinfrastrukturen und Prozessen politischer Mobilisierung.

6. Welche konkreten Anstrengungen hat die Bundesregierung in Vorbereitung auf die nationale Sicherheit der EU-Wahlen unternommen, etwa in Gestalt von Sicherheitsprogrammen von Akteuren im konkreten Wahlprozess, in Vorbereitung von Kommunikationsstrategien bei Zwischenfällen oder in Gestalt der Durchführung von Informationskampagnen in der Bevölkerung (zu gebotenen Maßnahmen nach Ansicht der Fragesteller instruktiv: Der Schutz von Wahlen in vernetzten Gesellschaften, Papier der Stiftung Neue Verantwortung, Oktober 2018)?

Bereits vor und nach der Bundestagswahl 2017 haben sich Ressorts und Nachrichtendienste eng in der Lageanalyse abgestimmt. Zur Gewährleistung der IT-Sicherheit der Bundestags- und Europawahlen besteht zwischen dem Bundeswahlleiter, den Landeswahlleitern und dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) ein enges Kooperationsverhältnis. Das BSI hat vor der Bundestagswahl 2017 und vor der Europawahl 2019 Parteien und politische Stiftungen zu Fragen der IT-Sicherheit beraten und wird dieses Angebot verstetigen.

Im Übrigen wird auf die Antworten der Bundesregierung auf die Schriftlichen Fragen 32 und 33 des Abgeordneten Alexander Graf Lambsdorff auf Bundestagsdrucksache 19/5155 und auf die Schriftliche Frage 27 der Abgeordneten Dr. Franziska Brantner auf Bundestagsdrucksache 19/6961, sowie auf die Antworten der Bundesregierung auf die Mündliche Frage 48 der Abgeordneten Renate Künast in der Fragestunde vom 16. Januar 2019 (Plenarprotokoll 19/73) und zu den Fragen 6, 7 und 10 der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 19/8056 sowie auf die Antwort auf die Schriftliche Frage 21 der Abgeordneten Dr. Franziska Brantner auf Bundestagsdrucksache 19/9360 verwiesen.

7. Welche internationalen Netzwerke, die illegitime Beeinflussung demokratischer Willensbildungsprozesse in Deutschland vorantreiben oder einsetzen, sind der Bundesregierung bekannt?

   Welche Reiseaktivität aus Deutschland hat die Bundesregierung in diesem Zusammenhang beobachten können?

8. Welche inländischen Gruppen oder Strukturen sind der Bundesregierung bekannt, die mit diesen internationalen Netzwerken in Verbindung stehen und zusammenarbeiten?

Die Fragen 7 und 8 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Maßnahmen zur illegitimen Beeinflussung demokratischer Willensbildungsprozesse sind in der Regel staatlichen und nichtstaatlichen Akteuren einzelner Staaten zuzuordnen. Darüber hinausgehende Erkenntnisse zu internationalen Netzwerken oder inländischen Gruppen bzw. Strukturen im Sinne der Fragestellungen sind der Bundesregierung nicht bekannt.

Auch über Verbindungen der bekannten inländischen Gruppierung „Reconquista Germanica“ zu internationalen Netzwerken im Sinne der Fragestellung liegen der Bundesregierung keine Erkenntnisse vor. Im Übrigen wird zu „Reconquista Germanica“ auf die Antworten der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/6562, auf die Schriftlichen Fragen 15

und 25 des Abgeordneten Ulrich Lechte auf Bundestagsdrucksachen 19/4634 und 19/4946 sowie auf die Kleinen Anfragen der Fraktionen DIE LINKE. auf Bundestagsdrucksache 19/1994 und BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/2224 verwiesen.

9. Hält die Bundesregierung auch angesichts der Tatsache, dass neue hybride Bedrohungslagen bereits in dem im Juli 2016 vorgestellten „Weißbuch der Bundesregierung zur Sicherheitspolitik und zur Zukunft der Bundeswehr" als eine zentrale sicherheitspolitische Herausforderung charakterisiert werden, bestehende Strukturen zur Erkennung derartiger Bedrohungen für ausreichend, und ist die Bundesregierung der Ansicht, dass eine wirksame ressortgemeinsame und gesamtstaatliche Sicherheitsvorsorge zur Unterbindung und Abwehr hybrider Angriffe derzeit gegeben ist?

   Welche Schritte wurden diesbezüglich bisher unternommen bzw. sind gegenwärtig in der Umsetzung oder Planung?

Es wird auf die Vorbemerkung der Bundesregierung unter Nummer 2 verwiesen.

10. Sollte die Bundesregierung bestehende Strukturen für nicht ausreichend erachten, wie will man sich national zukünftig besser aufstellen, und welche Rolle sollen hierbei Cyberabwehrzentrum (plus), das Bundesamt für Verfassungsschutz, das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr und der Beauftragte im Auswärtigen Amt für Cyber-Außenpolitik spielen?

Es wird auf die Vorbemerkung der Bundesregierung unter Nummer 2 Bezug genommen. Die Bundesregierung ist der Ansicht, dass hybride Bedrohungen nur durch einen regierungsweiten Ansatz effektiv erkannt und bekämpft werden können, der bestehende Strukturen gemäß dem jeweils geltenden Rechtsrahmen effektiv einbindet, wie unter anderem die vom Fragesteller genannten Stellen und Behörden.

11. Sollte die Bundesregierung bestehende Strukturen für nicht ausreichend erachten, wie möchte sie sich in Zukunft europäisch besser aufstellen, und welche Rolle kommen hierbei den bei Europol angesiedelten Zentren gegen Cyberkriminalität sowie gegen Terrorismus oder dem Computersicherheits-Ereignis- und Reaktionsteam der EU (CERT-EU) jeweils zu?

Die Bundesregierung arbeitet mit den übrigen Mitgliedstaaten der EU und den EU-Institutionen zusammen, um die bestmögliche Aufstellung der EU in Hinblick auf hybride Bedrohungen zu erreichen. Die Bundesregierung befürwortet auch auf EU-Ebene grundsätzlich den Einsatz und die Vernetzung vorhandener Expertise in Bezug auf hybride Bedrohungen im Rahmen der Zuständigkeiten der jeweiligen Einrichtungen.

12. Welche konkreten Schritte hat die Bundesregierung bisher und wird sie in Zukunft auf internationaler Ebene unternehmen, um einen besseren Schutz vor Desinformationskampagnen und der Beeinflussung von demokratischen Prozessen zu erreichen?

Desinformation ist eine transnationale Herausforderung, der kein Staat alleine effektiv begegnen kann. Die Bundesregierung ist daher in verschiedenen Formaten vertreten, die einem intensiveren Austausch zum Umgang mit Desinformation dienen. So trägt die Bundesregierung aktiv zum Frühwarnsystem zu Desinformation der EU (Rapid Alert System) bei, welches Anfang 2019 eingerichtet wurde.

Sie setzte sich ebenfalls für die Einrichtung der horizontalen Arbeitsgruppe „Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats" ein, die sich mit hybriden Gefährdungen und Desinformation befasst und seit Juli 2019 etabliert ist. Auch in anderen Foren, beispielsweise innerhalb des G7 Rapid Response Mechanisms, setzt sich die Bundesregierung für eine verstärkte Vernetzung und den Austausch von Informationen und „best practices" zum Umgang mit Desinformation ein.

a) Welche internationalen Regeln und Vereinbarungen will die Bundesregierung erreichen?

Die Europäische Kommission hat mit der Mitteilung „Bekämpfung von Desinformation im Internet: Ein europäisches Konzept" vom 26. April 2018 einen umfassenden Maßnahmenkatalog vorgelegt, der verschiedenste Akteure wie EU-Mitgliedstaaten, Online-Plattformen und Medienunternehmen einbezieht. In Ergänzung dieses europäischen Konzepts haben sich Online-Plattformen und Industrieverbände aus Kommunikation und Werbung Ende September 2018 einen Verhaltenskodex zur Selbstregulierung auferlegt, mit dem sie sich u. a. zur Bekämpfung von Online-Desinformation verpflichten. Die EU-Kommission wird Ende 2019 eine umfassende Bewertung der erzielten Fortschritte vornehmen und ggf. weitere Maßnahmen vorschlagen, die auch regulatorische Maßnahmen beinhalten können. Die Bundesregierung unterstützt die Aktivitäten der EU-Kommission im Hinblick auf eine Umsetzung des Verhaltenskodex, um effektive Maßnahmen gegen Desinformation zu treffen und eine größere Transparenz für die Nutzer zu erreichen.

b) Welche diesbezüglichen Initiativen plant die Bundesregierung im Rahmen der gegenwärtigen Mitgliedschaft im Sicherheitsrat der Vereinten Nationen?

Die Bundesregierung plant derzeit keine Initiativen zum Schutz vor Desinformationskampagnen und der Beeinflussung von demokratischen Prozessen im Sicherheitsrat der Vereinten Nationen.

c) Plant die Bundesregierung, das Thema auch im Rahmen des dieses Jahr in Deutschland stattfindenden Internet Governance Forums zu thematisieren?

Falls ja, in welcher konkreten Form, und falls nicht, warum nicht?

Das konkrete Programm des Internet Governance Forums (IGF) wird nicht von der Bundesregierung, sondern von der Multistakeholder Advisory Group (MAG) festgelegt, welche aus über fünfzig vom Generalsekretär der Vereinten Nationen ernannten Vertreterinnen und Vertretern aus Zivilgesellschaft, Wirtschaft, Regierungen und Fachöffentlichkeit besteht. Von ihr wurden auch die drei Schwerpunktthemen des IGF 2019 (Data Governance, Digital Inclusion und Security, Safety, Stability, Resilience) festgelegt. Das Schwerpunktthema Security, Safety, Stability, Resilience beinhaltet die Thematik der Desinformation sowie die Beeinflussung von demokratischen Prozessen, was sich in entsprechenden Workshops und Panels der Konferenz widerspiegelt (z. B. Workshop 85 „Misinformation, Trust & Platform Responsibility" und 218 „Deliberating Governance Approaches to Disinformation").

13. Welche Bundesministerien, Behörden und Stellen sollen an der Erkennung und Abwehr hybrider Bedrohungen nach dem Willen der Bundesregierung beteiligt sein (bitte auflisten), und wie wird die Bundesregierung ein rechtsstaatliches und verlässlichen Zusammenwirken dieser gewährleisten?

Es wird auf die Vorbemerkung der Bundesregierung unter Nummer 2 sowie auf die Antwort zu Frage 10 Bezug genommen. An der Erkennung und Abwehr hybrider Bedrohungen sollen nach dem regierungsweiten Ansatz grundsätzlich alle Ministerien und Behörden beteiligt werden. Das rechtsstaatliche Zusammenwirken wird durch den gültigen Rechtsrahmen sichergestellt. Das verlässliche Zusammenwirken wird durch eine zentrale Koordinierung durch das federführende Ministerium gefördert.

14. Wie beurteilt die Bundesregierung die Arbeit des NATO Cooperative Cyber Defence Centres in der Abwehr hybrider Bedrohungen, und in welcher Weise fließen die Ergebnisse der Arbeit des Zentrums in die deutsche Sicherheitsvorsorge ein?

Das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) trägt zur Entwicklung eines besseren Verständnisses in Bezug auf hybride Bedrohungen bei. Dies umfasst sowohl rechtliche als auch Verfahrensfragen, wie ggf. auf Bedrohungen reagiert werden kann.

Arbeitsergebnisse, Erkenntnisse und Produkte (z. B. Allied Joint Publication, Tallinn Manual 2.0 usw.) des NATO CCDCOE werden bei der Erstellung nationaler Vorgaben und Produkte berücksichtigt. Je nach Ergebnis kann dieses im Rahmen der etablierten Prozesse auch in die gesamtstaatliche Sicherheitsvorsorge einfließen.

15. In welcher Weise hat sich die Bundesregierung an der NATO-Übung Locked Shields 2019 beteiligt, und wenn ja, mit welchen Ergebnissen?

Die Bundeswehr hat sich mit 47 Teilnehmern an der Übung Locked Shields 2019 beteiligt. Das Ziel der Übung, die Fähigkeiten der Übungsteilnehmer im Zusammenhang mit der Bewältigung von Cyber-Angriffen zu trainieren und zu verbessern, wurde erreicht.

16. Hat die Bundesregierung bereits in allen Ressorts, in deren Zuständigkeit mögliche Einzelmaßnahmen zur Abwehr komplexer hybrider Bedrohungen liegen, Kopfstellen benannt, die im Eventualfall eine schnelle gesamtstaatliche Reaktion ermöglichen (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388)?

Falls ja, in welchen Bundesministerien genau?

Falls nein, warum noch nicht, und in welchen Ressorts aus welchem konkreten Grund noch nicht?

Es wird auf die Antwort zu Frage 13 verwiesen.

17. Bleibt die Bundesregierung bei ihrer Ansicht, dass vor allem die „frühzeitige Aufklärung einer hybriden Bedrohung sowie die Stärkung von Resilienz“ von entscheidender Bedeutung sind (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9388), um auf neue Bedrohungslagen angemessen reagieren zu können?

    Falls ja, wie passt das mit derzeitigen Plänen der Bundesregierung zusammen, die das Ziel verfolgen, offensive Kapazitäten zu stärken und digitale Gegenschläge und sogenannte Hackbacks zu ermöglichen?

Die Bundesregierung ist weiterhin der Ansicht, dass die Unterbindung und Abwehr hybrider Angriffe eine wirksame ressortgemeinsame und gesamtstaatliche Sicherheitsvorsorge erfordert. Diese beinhaltet vor allem die Stärkung von Resilienz sowie die frühzeitige Aufklärung einer hybriden Bedrohung.

Auch im Cyber-Raum ist für die Bundesregierung die Stärkung der Resilienz ein zentraler und wirksamer Baustein eines ganzheitlichen Cyber-Sicherheitsansatzes. Dennoch sind schwerwiegende Cyber-Angriffe vorstellbar, gegen die Maßnahmen der passiven Cyber-Abwehr allein keinen hinreichenden Schutz bieten könnten. Die Bundesregierung prüft daher die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen.

18. Sind durch die Bundesregierung oder ihr unterstellte Behörden bereits sogenannte Hackbacks durchgeführt worden (wenn ja, bitte auflisten nach Art des Angriffs, Attribution, Zeitpunkt der Attribution, Auswahl des Ziels, beteiligten Behörden und Art der Beteiligung)?

Es wird auf die Antwort der Bundesregierung zu Frage 17 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/2643 verwiesen.

19. Bleibt die Bundesregierung bei der bislang von ihr vertretenen Meinung, dass es für derartige Hackbacks keines Mandats des Deutschen Bundestages bedarf, dies vielmehr nur im jeweiligen Einzelfall entschieden werden kann (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420)?

    Falls ja, wer entscheidet im Einzelfall?

Bezüglich des Einsatzes der Bundeswehr wird auf die Antwort zu Frage 12 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420 verwiesen.

„Militärische Maßnahmen im Cyber-Raum unterliegen dem gleichen rechtlichen Rahmen wie andere militärische Maßnahmen auch. Nach dem Parlamentsbeteiligungsgesetz unterliegen bewaffnete Einsätze der Streitkräfte außerhalb des Geltungsbereichs des Grundgesetzes grundsätzlich der vorherigen konstitutiven Zustimmung des Deutschen Bundestages. Ob ein Vorgehen der Bundeswehr im Cyber-Raum diese Voraussetzung erfüllt, kann nur für den jeweiligen Einzelfall entschieden werden.“

Die Entscheidung erfolgt jeweils nach den für den Einzelfall gültigen Verfahren zum Einsatz militärischer Maßnahmen.

20. Ist im Hinblick auf die „aktive Abwehr“ von IT-Angriffen der Prüfvorgang innerhalb der Bundesregierung zur Frage, wie man mit der Attributions-Problematik bei IT-Angriffen und ihrer Abwehr umzugehen gedenkt, bereits abgeschlossen (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420)?

    Falls ja, mit welchem Ergebnis?

Der Prüfvorgang ist innerhalb der Bundesregierung noch nicht abgeschlossen.

21. Welche Versuche einer illegitimen Einflussnahme durch ausländische staatliche und nichtstaatliche Akteure hat es nach Kenntnis der Bundesregierung bei Wahlgängen in Deutschland seit September 2013 gegeben?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor.

22. Welche Versuche illegitimer Einflussnahme durch ausländische staatliche und nichtstaatliche Akteure hat es nach Kenntnis der Bundesregierung bei Wahlkämpfen in Deutschland seit September 2013 gegeben?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor.

23. Teilt die Bundesregierung die Ansicht der Fragesteller, dass die Stärkung von Resilienz nur dadurch zu erreichen sein wird, die eigene IT-Sicherheitspolitik grundlegend zu überdenken und beispielsweise bestehende Sicherheitslücken schnellstmöglich im Zusammenspiel von staatlichen Stellen und Privatwirtschaft zu schließen, und wenn nein, warum nicht?

Für eine grundlegende Änderung der IT-Sicherheitspolitik sieht die Bundesregierung keinen Anlass. Die Stärkung der Resilienz ist für sie bereits heute ein zentraler und wirksamer Baustein eines ganzheitlichen Cyber-Sicherheitsansatzes. Mit dem BSI unterhält die Bundesregierung eine Bundesbehörde, die für die Informationssicherheit auf nationaler Ebene zuständig ist und die Sicherheit in der Informationstechnik fördert – mithin die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen sicherstellen. Mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 wurden Vorgaben zur Steigerung der Resilienz insbesondere auch im Bereich der Wirtschaft gesetzliche Pflicht. Bei der Umsetzung der mit dem IT-Sicherheitsgesetz eingeführten Mindestanforderungen und Meldepflichten arbeiten Staat und Wirtschaft vertrauensvoll und eng zusammen, unter anderem im Rahmen der öffentlich privaten Partnerschaft des UP KRITIS. Auch mit dem Umsetzungsgesetz zur NIS-Richtlinie wurde die IT-Sicherheit in Deutschland weiter erhöht. So wurden beispielsweise Regelungen für den Einsatz der sogenannten „Mobilen Incident Response Teams“ (MIRTs) des BSI geschaffen. Diese Teams können Verfassungsorgane, Bundesbehörden sowie Betreiber Kritischer Infrastrukturen und vergleichbar wichtiger Einrichtungen auf Ersuchen vor Ort schnell, flexibel und adressatengerecht bei der technischen Bewältigung von Sicherheitsvorfällen unterstützen. Mit der „Cyber-Sicherheitsstrategie für Deutschland 2016“, die übergreifende Zielstellungen für alle Bereiche und Akteure in der IT-Sicherheit beinhaltet, legt die Bundesregierung erneut einen deutlichen Schwerpunkt auf die Steigerung der Resilienz von IT-Infrastrukturen. Die Bundesregierung strebt zudem an, noch in dieser Legislaturperiode ein IT-Sicherheitsgesetz 2.0 auf den Weg zu bringen, das weitere Maßnahmen für den Schutz der Bürgerinnen und Bürger, der Wirtschaft und des Staates im Cyber-Raum enthalten wird.

24. Ist die entsprechende Prüfung innerhalb der Bundesregierung bereits abgeschlossen, und wenn ja, was ist das konkrete Ergebnis, und plant die Bundesregierung, nunmehr eine Meldepflicht für Sicherheitslücken für staatliche Stellen zu schaffen (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420), und wenn nein, warum nicht?

Die Bundesregierung setzt sich inhaltlich mit dem Thema auseinander einen geregelten Prozess zu schaffen, der dem Anliegen der IT-Sicherheit genauso Rechnung trägt wie den Erfordernissen der Strafverfolgungs- und Sicherheitsbehörden. Die Meinungsbildung innerhalb der Bundesregierung hierzu ist nicht abgeschlossen. Es wird ferner auf die Antworten der Bundesregierung auf die Schriftliche Frage 25 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/13696 sowie zu Frage 21 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/1867 verwiesen.

25. Welche Anstrengungen hat die Bundesregierung bislang mit welchen Staaten unternommen, um zu einem Capacity Building zur weltweiten Schließung von Sicherheitslücken zu kommen?

Die Bundesregierung unternimmt im Ausland aktuell keine Kapazitätsaufbaumaßnahmen hinsichtlich der Schließung von Sicherheitslücken.

26. Welche Pläne hat die Bundesregierung für die anstehende EU-Ratspräsidentschaft im Hinblick auf die Stärkung des EU-Rahmens gegen hybride Bedrohungen?

Die Planungen der Bundesregierung für die anstehende EU-Ratspräsidentschaft sind noch nicht abgeschlossen. Im Hinblick auf die Stärkung des EU-Rahmens gegen hybride Bedrohungen plant die Bundesregierung grundsätzlich die Fortführung der Vorhaben in der „Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats“ entsprechend deren Mandats und der unter finnischen und kroatischen Vorsitz geleisteten Arbeiten.

27. Bleibt die Bundesregierung bei der bisher vertretenen Ansicht, dass Schwachstellen, deren Nutzung weitreichende Auswirkungen auf die Sicherheit der Bevölkerung bzw. des Staates haben, auch durch staatliche Stellen gemeldet werden sollen, andere aber nicht (vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/3420), und wer soll nach Ansicht der Bundesregierung zukünftig prüfen und entscheiden, ob dies für eine entdeckte Lücke zutrifft oder nicht, und wie kann eine solche Entscheidung nach Ansicht der Bundesregierung gerichtlich überprüft und parlamentarisch kontrolliert werden?

Auf die Antwort zu Frage 24 wird verwiesen.

28. Welche Szenarien und Maßnahmen sind während der „Live-Fire-Cyber-Abwehr Übung“ Locked Shields 2019 vom 9. bis 12. April 2019 des NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn/Estland zur „Abwehr von Fake News“ geplant oder geübt worden, an denen sich die Bundeswehr beteiligte (vgl. https://cir.bundeswehr.de/portal/poc/cir?uri=ci%3Abw.cir.service.archiv.2019.apr&de.conet.contentintegrator.portlet.current.id=01DB160000000001%7CBAXA9Q092DIBR)?

Das NATO CCDCOE in Tallinn/Estland nutzte während der Übung Locked Shields 2019 ein Szenario, in dem Falschnachrichten zur Desinformation, Verunsicherung und Aufwiegelung der Bevölkerung eingesetzt wurden. Dem begegneten die Übungsteilnehmer mit aktiven Informationen und Richtigstellungen über Social-Media-Kanäle und Pressemitteilungen sowie reaktiv bei telefonischen Presseanfragen.

29. Welche Rolle kann und sollte die Bundeswehr nach Auffassung der Bundesregierung in der Abwehr von „Desinformation“ spielen?

Das BMVg und die Bundeswehr kommen im Rahmen des grundgesetzlichen Auftrages und ihrer Informationspflicht mit einem breiten Spektrum von digitalen und analogen Informationsangeboten nach. Diese bieten politisch interessierten Bürgerinnen und Bürgern die Möglichkeit, sich ein eigenes Bild zu unterschiedlichen Sachverhalten zu machen. Dabei sind für BMVg und Bundeswehr lediglich diejenigen Themen relevant, die den eigenen Aufgabenbereich betreffen.

In mandatierten Einsätzen ist es unter anderem eine der Aufgaben der Bundeswehr, die eigenen Soldatinnen und Soldaten zu schützen. Mit Blick auf Desinformation geschieht dies durch die Analyse der Lage im Informationsumfeld, die Analyse von Propaganda/Desinformation sowie die erforderliche Information der eigenen Truppe.

Ist es für die Durchführung des Einsatzes relevant, wird der Desinformation durch geeignete eigene Informationsaktivitäten, auch zur Information der Bevölkerung in den Einsatzgebieten, begegnet.

Darüber hinaus können Beiträge zur gesamtstaatlichen Analyse und dem gesamtstaatlichen Lagebild durch das Bereitstellen von Analyseprodukten und gegebenenfalls Handlungsempfehlungen zum Informationsumfeld durch die Bundeswehr erfolgen.

30. Welche rechtlichen Befugnisse hat die Bundeswehr nach Auffassung der Bundesregierung, um gegen die Verbreitung von Informationen und Desinformationen im Inland oder im Ausland vorzugehen?

Die rechtlichen Vorgaben für jedwedes Tätigwerden der Bundeswehr ergeben sich aus den einschlägigen Bestimmungen des Grundgesetzes und – insbesondere bei einem Handeln im Ausland – aus den jeweils geltenden völkerrechtlichen Rahmenbedingungen.

31. Welche Erkenntnisse hat die Bundesregierung zu Anwerbungs- und Infiltrationsversuchen von Mandatsträgerinnen und Mandatsträgern und Kandidatinnen und Kandidaten für öffentliche Ämter in Deutschland durch ausländische Nachrichtendienste?

Generell zählen Mandatsträgerinnen und -träger sowie Kandidatinnen und Kandidaten für öffentliche Ämter in Deutschland zu den hochwertigsten Zielen ausländischer Nachrichtendienste, sowohl im Hinblick auf die Abschöpfung relevanter Informationen als auch in Bezug auf die Möglichkeiten einer Einflussnahme.

Nach Kenntnis der Bundesregierung nutzen gerade chinesische Nachrichtendienste soziale Netzwerke, insbesondere LinkedIn, zur Anwerbung nachrichtendienstlicher Quellen. Im Fokus können neben Bundestagsabgeordneten (sowie deren Mitarbeitern) insbesondere Mitarbeiter deutscher und europäischer Behörden, Diplomaten, Angehörige der Bundeswehr und der NATO, Wissenschaftler, freie Politikberater aber auch Studenten und Mitarbeiter deutscher Stiftungen stehen.

a) Wie viele Fälle von Anwerbungs- und Infiltrationsversuchen von Bundestagsabgeordneten durch ausländische Nachrichtendienste in den letzten fünf Jahren sind der Bundesregierung bekannt (bitte nach Staat, Parteizugehörigkeit, Art und Intensität der Einflussnahme aufschlüsseln)?

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage 31a aus Staatswohlgründen nicht beantwortet werden kann. Die in dieser Frage erbetenen Angaben können aus Gründen des Methoden- und Quellenschutzes nicht mitgeteilt werden, weil sie auf Informationen basieren, die im Zusammenhang mit der Arbeitsweise und Methodik der Verfassungsschutzbehörden und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik der Sicherheitsbehörden – hier zum Erkenntnisstand des Bundesamtes für Verfassungsschutz (BfV) – einem nicht eingrenzbaren Personenkreis zugänglich machen. So könnten aus der Antwort Rückschlüsse auf die generelle Arbeitsweise des BfV und Rückschlüsse auf den Erkenntnisstand sowie Aufklärungsbedarf des BfV gezogen werden.

Das Risiko des Bekanntwerdens auf Seiten der ausführenden Nachrichtendienste und der Möglichkeit der dortigen Analyse und Rückschlüsse auf erfolgreiche und/oder fehlgeschlagene Anwerbungsversuche sowie der damit einhergehenden Schädigung deutscher Interessen ist aus Gründen des Staatswohls unbedingt zu vermeiden. Es würde die Gefahr entstehen, dass bestehende oder in der Entwicklung befindliche operative Fähigkeiten und Methoden des BfV aufgeklärt und damit der Einsatzerfolg gefährdet würden. In der Folge könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland bedeuten. Die erbetenen Informationen berühren insofern derart schutzwürdige Geheimhaltungsinteressen, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt.

Im vorliegenden Fall kann das Staatswohlinteresse an der Geheimhaltung auch nicht durch eine VS-Einstufung der Antwort gewährleistet werden. Somit kann im Zuge einer Gesamtschau und unter sorgfältiger Abwägung der widerstreitenden Interessen selbst ein geringfügiges Risiko des Bekanntwerdens nicht hingenommen werden. Dies kann jedoch nur gewährleistet werden, wenn eine Stellungnahme zu der gestellten Frage nicht erfolgt.

b) Wie viele Ermittlungsverfahren hat der Generalbundesanwalt wegen der §§ 94 ff. des Strafgesetzbuchs in den letzten fünf Jahren im Zusammenhang mit Mandatsträgerinnen und Mandatsträgern und Kandidatinnen und Kandidaten für öffentliche Ämter geführt (bitte in Bezug auf Staaten und Parteizugehörigkeit aufschlüsseln)?

Die Bundesregierung nimmt keine Stellung zu eventuell geführten Ermittlungsverfahren des Generalbundesanwalts beim Bundesgerichtshof wegen der §§ 94 ff. des Strafgesetzbuchs in den letzten fünf Jahren im Zusammenhang mit Mandatsträgern/Mandatsträgerinnen und Kandidaten/Kandidatinnen für öffentliche Ämter. Schon eine Auskunft, ob überhaupt solche Verfahren geführt wurden beziehungsweise werden, könnte (auch in künftigen Fällen) die Ermittlungen beeinträchtigen. Daher tritt nach Abwägung im konkreten Einzelfall das Informationsinteresse des Parlaments hinter berechtigte Strafverfolgungsinteressen zurück.

32. Welche eigenen Erkenntnisse hat die Bundesregierung über „materielle und mediale Unterstützung" von Bundestagsabgeordneten durch Russland (vgl. DER SPIEGEL, 6. April 2019), und wie ordnet sie eine solche mögliche Unterstützung rechtlich ein?

Die Bundesregierung nimmt mögliche unzulässige Einflussnahmen auf Abgeordnete des Deutschen Bundestages sehr ernst. Nach Erkenntnissen der Bundesregierung versucht Russland im Rahmen seiner Einflussstrategie, Politiker und politische Bewegungen unabhängig von ihrer ideologischen Ausrichtung zu unterstützen bzw. zu fördern. Ein einendes Element bei den ausgesuchten Akteuren besteht darin, dass die Politiker und politischen Bewegungen russische Positionen oder solche, die im Interesse Russlands sind (z. B. Aufhebung der Sanktionen, Akzeptanz der Annexion der Krim), vertreten. Belastbare Erkenntnisse für solche konkreten unzulässigen russischen Einflussnahmen im Sinne der in der Frage zitierten Medienberichterstattung, insbesondere durch russische Nachrichtendienste, auf Bundestagsabgeordnete oder die Unterstützung einzelner Bundestagskandidaten, etwa zur Förderung ihrer Wahlchancen im Zusammenhang mit der Bundestagswahl 2017, liegen der Bundesregierung bislang nicht vor. Die geschilderten Sachverhalte fügen sich aber plausibel in das Bild russischer Einflussnahme-Aktivitäten in Deutschland und Europa ein.

33. Inwiefern sind der Bundesregierung Einflussnahmeversuche von anderen Staaten als Russland auf Bundestagsabgeordnete bekannt?

Der Bundesregierung liegen Erkenntnisse über Einflussnahmeversuche von anderen Staaten als Russland auf Bundestagsabgeordnete vor. Auf die Antwort zu Frage 31 wird verwiesen.

34. Welche Erkenntnisse hat die Bundesregierung zu Anwerbungs- und Infiltrationsversuchen von Mitarbeitern von Abgeordneten im Deutschen Bundestag durch ausländische Nachrichtendienste, und wie viele Fälle in den letzten fünf Jahren sind der Bundesregierung bekannt (bitte nach Staat, Fraktionszugehörigkeit, Art und Intensität der Einflussnahme aufschlüsseln)?

Auf die Antworten zu den Fragen 31 und 31a wird verwiesen.

35. Wie oft haben Bundestagsabgeordnete während der 19. Wahlperiode für Reisen nach Russland die diplomatischen Institutionen der Bundesrepublik Deutschland um Unterstützung gebeten bzw. vorab konsultiert (bitte nach Fraktionen aufschlüsseln)?

Seit Beginn der 19. Legislaturperiode haben insgesamt 29 Delegationen mit Beteiligung eines oder mehrerer Bundestagsabgeordneten im Rahmen von Reisen nach Russland das Auswärtige Amt, die Botschaft Moskau und/oder die Generalkonsulate um Unterstützung gebeten bzw. konsultiert.

36. Gibt es in der Bundesregierung eine Stelle, die für die Identifizierung von durch ausländische Regierungen gesteuerte Medienunternehmen in Deutschland zuständig ist, und wenn ja, welche?

Die Bundesregierung als Ganzes beobachtet bei der Erfassung möglicher ausländischer Einflussnahme auch die in Deutschland agierenden ausländischen bzw. mutmaßlich aus dem Ausland gesteuerten Medien.

37. Hat die Bundesregierung über die in der Kleinen Anfrage „Rechtspopulismus, Rechtsextremismus und Politische Desinformation im Netz“ (Bundestagsdrucksache 19/2224, Frage 25) genannten hinausgehende Erkenntnisse über von ausländischen Regierungen gesteuerte Medienunternehmen, welche gezielt in Deutschland Desinformationen verbreiten?

Im Internet bemühen sich im besonderen Maß zwei russische Staatsmedien um eine Beeinflussung der Öffentlichkeit. Es handelt sich hierbei um das Internetfernsehen Russia Today (RT) Deutsch und die Nachrichtenagentur Sputnik (auch: Sputniknews). Diese fielen 2016 durch eine Desinformationskampagne im so genannten Fall „Lisa“ auf und waren daraufhin einer massiven öffentlichen Kritik ausgesetzt.

Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 1 und 2 der Kleinen Anfrage der Fraktion der FDP „Mögliche russische Einflussnahme auf öffentliche Meinung in Deutschland“ auf Bundestagsdrucksache 19/6562 sowie auf die Antwort zu Frage 14 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN „Rechtspopulismus, Rechtsextremismus und Politische Desinformation im Netz“ auf Bundestagsdrucksache 19/2224 verwiesen.

38. Welche Strategie hat die Bundesregierung, insbesondere in Zusammenarbeit mit den Bundesländern, zur Verhinderung von gezielter Desinformation durch von ausländischen Regierungen gesteuerte Medienunternehmen?

39. Vertritt die Bundesregierung die Ansicht, dass die Aufsicht der Medien verbessert werden muss in Anbetracht der Gefahr von Desinformation durch von ausländischen Regierungen gesteuerte Medienunternehmen, und wenn ja, durch welche Maßnahmen?

Die Fragen 38 und 39 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Werden Desinformationen über die journalistisch-redaktionellen Medien verbreitet, besteht die Möglichkeit, je nach Verbreitungsweg den Presserat, den Rundfunkrat oder die Landesmedienanstalten wegen der Verletzung journalistischer Sorgfaltspflichten anzurufen oder gegebenenfalls auf Grundlage der geltenden Gesetze, unter anderem der Vorschriften des Strafgesetzbuches, eine entsprechende Veröffentlichung zu ahnden.

Eine über diesen weitgehend selbstregulatorischen Ansatz hinausgehende gesetzliche Regulierung der Verbreitung von Desinformationen bedarf vertiefter Prüfung, da insbesondere nicht über Gebühr in die Meinungs-, Presse- und Rundfunkfreiheit eingegriffen werden darf.

40. Wie beurteilt die Bundesregierung Berichte über gezielte Einflussnahmen Chinas, die der ehemalige Präsident des Verfassungsschutzes Hans-Georg Maaßen als „breit angelegten Versuch der Infiltration insbesondere von Parlamenten, Ministerien und Behörden“ bezeichnet hat (vgl. ntv.de vom 6. Juli 2018 „Agenten Chinas in Deutschland Spione infiltrierten offenbar den Bundestag“, abrufbar unter www.n-tv.de/politik/Spione-infiltrierten-offenbar-den-Bundestag-article20516278.html)?

    a) Welche Strategien und Formen der Beeinflussung einzelner Mandatsträger und der Mitarbeiter von Behörden sind nach Kenntnis der Bundesregierung Teil dieser chinesischen Strategie?

Die Fragen 40 und 40a werden wegen des Sachzusammenhangs zusammen beantwortet.

Auf die Antwort zu Frage 31 und ergänzend die Ausführungen im Verfassungsschutzbericht 2018 (S. 296 ff.) wird verwiesen.

    b) Welche Rolle spielt nach Kenntnis der Bundesregierung gezielte Falschinformation zu Gunsten Chinas?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor.

    c) Welche Intentionen und konkreten Interessen verfolgen chinesische Sicherheitsbehörden nach Ansicht der Bundesregierung mit diesen gezielten Einflussnahmen?

Mit den beschriebenen Einflussnahmeversuchen erhoffen sich die chinesischen Nachrichtendienste nichtöffentliche Informationen über politische und gesellschaftliche Entwicklungen und Entscheidungsprozesse zu gewinnen und ggf. zu beeinflussen.

    d) Sind nach Kenntnis der Bundesregierung alle Fraktionen des Deutschen Bundestages von solchen Versuchen der Einflussnahme in gleichem Maß betroffen?

Nach Kenntnis der Bundesregierung waren nahezu alle im Deutschen Bundestag vertretenen Fraktionen in etwa gleichem Maße von chinesischen Einflussnahmeversuchen mittels sozialer Netzwerke betroffen.

41. Hält die Bundesregierung den Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation, den die EU-Kommission im April 2018 mit zahlreichen Stakeholdern ausgehandelt hatte, für hinreichend, um die wichtigsten Parameter wie die Transparenz politischer Werbung, die Schließung von Scheinkonten und die Kennzeichnung für automatisierte Bots zu erreichen?

    Wenn nicht, welche zusätzlichen Maßnahmen möchte die Bundesregierung in Deutschland durchsetzen und in Zukunft auf europäischer Ebene anstreben (vgl. hierzu unter anderem die Antwort der Bundesregierung auf die Schriftliche Frage 27 der Abgeordneten Dr. Franziska Brantner auf Bundestagsdrucksache 19/6961)?

Aus Sicht der Bundesregierung sind die in dem Verhaltenskodex zur Bekämpfung von Desinformation vorgesehenen Maßnahmen der Online-Plattformen, darunter Facebook, Google und Twitter, zur Bekämpfung von Desinformation sinnvoll. Ob und welche weiteren Maßnahmen erforderlich sind, hängt vor allem von der weiteren Umsetzung ab. Die EU-Kommission wird noch im Jahr 2019 die Wirksamkeit des Kodex bewerten. Sollten die Ergebnisse dieser Bewertung nicht zufriedenstellend ausfallen, kann die Kommission weitere Maßnahmen vorschlagen, einschließlich Maßnahmen rechtlicher Natur. Die Bundesregierung wird sich an dieser Diskussion aktiv beteiligen.

42. Inwieweit wird nach Kenntnis der Bundesregierung der Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation, den die EU-Kommission im April 2018 mit zahlreichen Stakeholdern ausgehandelt hatte, in Deutschland und in anderen europäischen Mitgliedstaaten umgesetzt?

    Wann und wie hat die Bundesregierung der EU-Kommission die Informationen über die Umsetzung des Verhaltenskodex für die Selbstregulierung im Bereich Online-Desinformation bereitgestellt, und welche Schlussfolgerungen ergeben sich im Hinblick auf die Integrität der Europawahl 2019 aus dem Bericht der Bundesregierung?

Die EU-Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik haben in ihrer Gemeinsamen Mitteilung vom 14. Juni 2019 an das Europäische Parlament, den Europäischen Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Umsetzung des Aktionsplans gegen Desinformation berichtet.

Der Bericht enthält auch ausführliche Informationen zur Umsetzung des Verhaltenskodex zur Bekämpfung von Desinformation (vgl. Dokument JOIN (2019) 12 final).

Der Verhaltenskodex wurde im Rahmen einer Selbstverpflichtung durch die beteiligten Online-Plattformen umgesetzt. Dieser Prozess wurde von der EU-Kommission begleitet. Die sich selbstverpflichteten Online-Plattformen berichteten direkt an die EU-Kommission. Eine Berichtspflicht der EU-Mitgliedstaaten ist im Verhaltenskodex nicht vorgesehen. Im Übrigen wird auf die Antwort zu Frage 12a Bezug genommen.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333